Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch

Shihan Sajeed,[1,2,*] Poompong Chaiwongkhot,[1,3] Jean-Philippe Bourgoin,[1,3]
Thomas Jennewein,[1,3,4] Norbert Lütkenhaus,[1,3] and Vadim Makarov[1,3,2]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

(Dated: June 11, 2015)

In free-space quantum key distribution (QKD), the sensitivity of the receiver's detector channels may depend differently on the spatial mode of incoming photons. Consequently, an attacker can control the spatial mode to break security. We experimentally investigate a standard polarization QKD receiver, and identify sources of efficiency mismatch in its optical scheme. We model a practical intercept-and-resend attack and show that it would break security in most situations. We show experimentally that adding an appropriately chosen spatial filter at the receiver's entrance may be an effective countermeasure.

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2], in theory, allows two distant parties Alice and Bob to establish a shared secret key with unconditional security [3–7]. Although a number of successful implementations of QKD have been reported [8–11] and commercialization is underway [12], the technology is yet to achieve widespread use. One important reason is that the maximum distance is still of the order of 300 km [13] in fiber-based systems. Consequently, implementation of free-space QKD utilizing ground-to-satellite links [14–22] that promises long-distance quantum communication is now a very attractive field of research.

Implementation imperfections have enabled a number of successful attacks on QKD [23–31]. The main reason behind this is the deviation of the actual behaviour of the devices from the ideal expected behaviour. Thus, to guarantee the security, it is of utmost importance to scrutinize the practical device behaviours for possible deviations. One such source of deviation in free-space QKD can be the assumed symmetry of detection efficiency among all received quantum states in Bob's detector [28–30, 32, 33]. If a deviation from this assumption exists, an adversary Eve can send light to Bob in different spatial modes so that one of his detectors has a relatively higher probability of click than the other detector(s) [34]. In this way, she can exploit the mismatch in efficiency and make Bob's measurement outcome dependent on his measurement basis and correlated to Eve, which breaks the assumptions of typical security proofs. In this work, we investigate how crucial this can be to the security of QKD. (While finishing this paper, we became aware of a recent similar work [35].)

We study a receiver designed for polarization encoding free-space QKD, described in Sec. II. We test it in Sec. III by sending an attenuated laser beam to the receiver with various angle offsets and recording the relative detection probability in each channel, to find incidence angles with high efficiency mismatch. With these data, we show in Sec. IV by numerical modeling that an eavesdropper attack exists that enables Eve to steal the secret key. We discuss countermeasures in Sec. V and conclude in Sec. VI.

II. QKD SYSTEM UNDER TEST

A free-space QKD receiver typically employs a telescope to reduce the size of a collimated beam, followed by a non-polarizing beamsplitter to randomly choose between two measurement bases. It is followed by polarization beamsplitters and single-photon detectors to measure photons in the four states of polarization: horizontal (H), vertical (V), +45° (D), and −45° (A) [14–22]. The receiver we test is a prototype for a quantum communication satellite [36], operating at 532 nm wavelength [Fig. 1(a,c)]. Its telescope consists of a focusing lens L1 (diameter 50 mm, focal length $f = 250$ mm; Thorlabs AC508-250-A) and collimating lens L2 ($f = 11$ mm; Thorlabs A397TM-A). The collimated beam of $\lesssim 2$ mm diameter then passes through a 50:50 beamsplitter BS (custom pentaprism [36]) and pairs of polarization beamsplitters PBS1 and PBS2 (Thorlabs PBS121). PBS2 increases the polarization extinction ratio in the reflected arm of PBS1. Lenses L3 (Thorlabs PAF-X-18-PC-A) focus the four beams into 105 μm core diameter multimode fibers (Thorlabs M43L01) leading to single-photon detectors (Excelitas SPCM-AQRH-12-FC).

Long-distance free-space QKD receivers are multimode for two reasons. First, propagation of Alice's beam, initially single-mode, through a turbulent atmosphere splits it into multiple spatial modes [37]. Second, the finite precision and speed of real-time angular tracking of Alice's beam requires that Bob accepts multiple spatial modes

* ssajeed@uwaterloo.ca

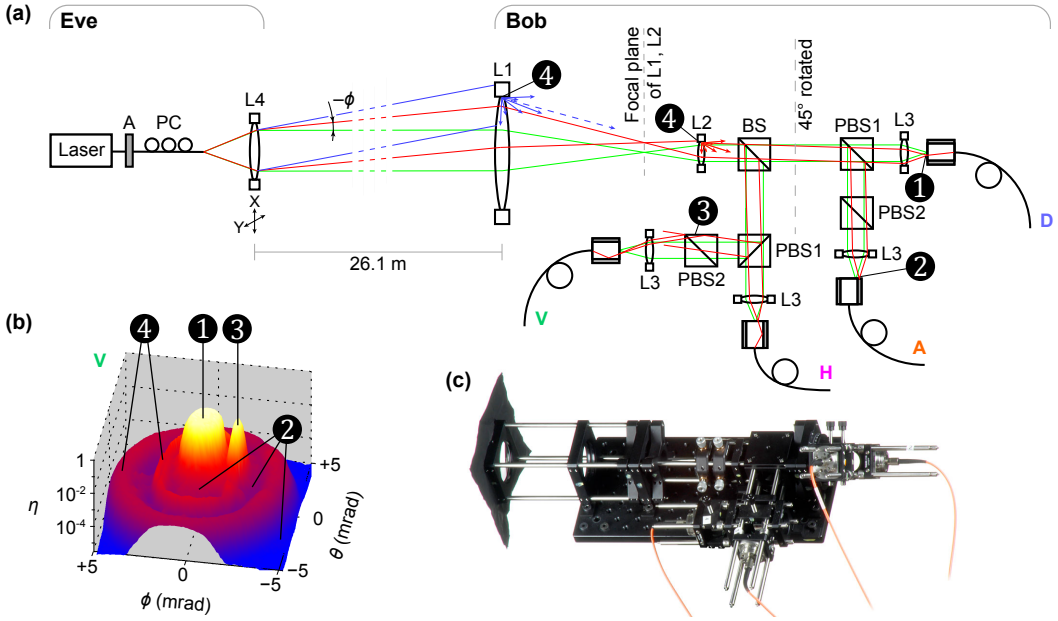

FIG. 1. (color online). Experimental setup. (a) Scheme of the experimental apparatus, top view (drawing not to scale). Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens mounted on a two-axis motorised translation stage. The latter allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. Green (light gray) marginal rays parallel to the optical axis denote the original alignment of Alice's beam to Bob. Red and blue (dark gray) marginal rays show a scanning beam from Eve tilted at an angle (ϕ, θ) relative to the original beam. Features ❶–❹ mark different transmission paths for light inside Bob. (b) Normalized detection efficiency η in channel V versus the illumination angle (ϕ, θ). This scan was taken to show the features clearly by placing Eve at a closer distance. (c) Photograph of Bob's receiver. The actual distance between facing surfaces of L2–BS is 42 mm, BS–PBS1 66 mm, PBS1–L3 31 mm, PBS1–PBS2 45 mm, PBS2–L3 10 mm in channel A and 5 mm in channel V.

in a certain acceptance angle [18, 19, 22, 38]. Use of single-mode fibers under these conditions would lead to additional coupling losses $\gtrsim 10$ dB [39] if the system does not include appropriate (and often expensive) adaptive correction optics [37]. Therefore, multimode fibers and detectors with larger area are generally preferred as they allow good collection efficiency without increasing complexity and cost.

III. EXPERIMENT

In order to exploit the mismatch in efficiency, Eve needs to know the mismatch for the four detectors as a function of the input angle. Hence, our first step was to scan Bob's receiver for possible efficiency mismatch. Eve's source [Fig. 1(a)] consists of a 532 nm laser coupled into single-mode fiber, attenuator A, polarization controller PC, and a collimating lens L4 (Thorlabs C220TME-A) mounted on a two-axis motorised translation stage (Thorlabs MAX343/M). In Fig. 1(a), green (light gray) marginal rays denote the initial alignment from Eve, replicating the alignment from Alice to Bob. This is the initial position of the translation stage $\phi = \theta = 0$. As we moved the stage in the transverse plane, it changed the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. This is shown by red (dark gray) marginal rays in Fig. 1(a), representing a beam from Eve coming at an angle (ϕ, θ) relative to the initial beam.

Before scanning, the optics in Bob's apparatus was aligned to maximize coupling into all four detectors at the normal incidence, which is the standard alignment procedure for QKD. Note that many free-space QKD systems employ a real-time tracking system to maintain this initial alignment [18, 19, 22, 38]. We then started the scanning procedure that involved first, changing the outgoing beam's angle (ϕ, θ), and then recording the corresponding count rate at all four detectors of Bob. For each data point, we used an integration time of 1 s. Our scan consisted of approximately 100×100 data points in a square matrix covering the whole clear aperture of Bob's front lens L1. Then during post-processing, for each data point for each detector, we subtracted the corresponding detector's background count rate, and then normalized it by dividing by the maximum count rate in that detector.

At first, we did a preliminary scan using optical power meters (Thorlabs PM200 with S130C head) that revealed several features, highlighted in Fig. 1(b). Around $\phi = \theta = 0$, maximum light coupling resulted in the central peak ❶. With increasing scanning angle, the focused beam started missing the fiber core, and the detector count dropped off ❷. A region was found when the beam reflected off a polished edge of PBS2 back into the

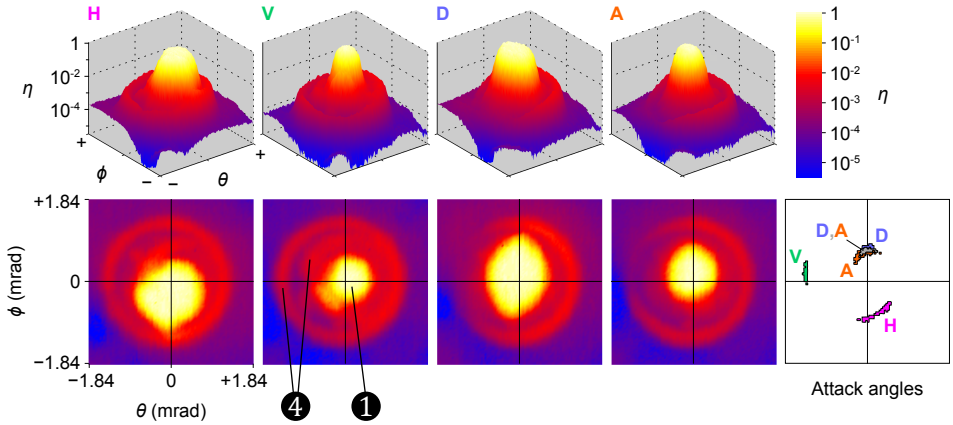

FIG. 2. (color online). Angular efficiency scan of the receiver, and points of interest. Four pair of plots **H, V, D, A** shown in both 3D and 2D represent normalized detection efficiency in the four receiver channels versus illuminating beam angle (ϕ, θ). The angle $\phi = \theta = 0$ is the initial angle of QKD operation. The last plot shows angle ranges with a high mismatch, usable in our attack.

fiber core, causing the peak ❸. Increasing the angle further made the beam hit the anodized aluminum mount of L1 and possibly edges of other lens mounts and round elements in the optical assembly. It was scattered at these edges, producing two ring-like features ❹. Beyond these features, there were no noticeable power reading, as the beam completely missed the receiver aperture.

We then adjusted the receiver setup to minimize the peak ❸, and performed final scans at 26.1 m distance using Bob's single-photon detectors (Excelitas SPCM-AQRH-12-FC). During these scans, the beam at L1 was Gaussian-shaped with 9 mm width (at $1/e^2$ peak intensity). The scans were done in 38.3 µrad steps covering ±1.84 mrad range, corresponding to lateral displacement of ±48 mm at L1. Figure 2 shows the normalized detection efficiency in all four receiver channels as a function of (ϕ, θ). Most of the original features are still visible. However, outside the narrow central range of angles close to $\phi = \theta = 0$, individual channel's efficiencies vary independently. Also, the size and shape of the central peak is significantly different between channels. This was impossible to identify during the normal alignment procedure. This effect can be attributed to imprecise focusing, optical path length difference between the arms, off-centered alignment of lenses, mode-dependent bending loss in fibers, and individual variations in components. These may have also caused the efficiency at one side of the outer ring being higher. Because of these reasons, there exist angles such that if photons are sent at those angles, one channel has a much higher click probability than the rest.

IV. ATTACK MODEL

To emphasize the security threat, it is useful to model an attack that exploits the discovered side-channel. One possible attack is the faked-state attack [30, 40], which is an intercept-and-resend attack in which Eve attempts to deterministically control Bob's basis choice and detection outcome. We model a practical faked-state attack using the obtained data and the following assumptions: Alice and Bob perform non-decoy-state Bennett-Brassard 1984 (BB84) protocol using polarization encoding. Alice emits weak coherent pulses with mean photon number μ equal to Alice–Bob line transmittance [5]. Whenever Bob registers a multiple click, he performs a squashing operation (double-click in one basis is mapped to a random value in that basis, while multiple clicks in different bases are discarded) [41–43]. Alice and Bob also monitor total sifted key rate, and quantum bit error ratio (QBER). Eve has information about Bob's receiver characteristics described above, and only uses devices available in today's technology. She intercepts photons at the output of Alice, using an active basis choice and superconducting nanowire detectors, with overall detection efficiency $\eta_e = 0.85$ and dark count probability $< 10^{-9}$ per bit slot [44]. Then, a part of her, situated close to Bob, regenerates the measured signal and sends to Bob. We assume that Alice–Bob and Alice–Eve fidelity $F = 0.9831$ [36], while Eve–Bob experimentally measured $F = 0.9904$. Here fidelity refers to the probability that a polarized photon will emerge from the PBS at the correct path, which is related to visibility by $F = (1 + \text{visibility})/2$. We also confirmed experimentally that Eve–Bob fidelity is preserved at all illumination angles shown in Fig. 2.

From Eve's point of view, she wants to maximize the detection probability when Bob measures in compatible (i.e., same as her) basis, to maximize Eve–Bob mutual information. Also, she wants to minimize Bob's detection probability in non-compatible basis, to minimize QBER. Let $\eta_i(j)$ be the efficiency of Bob's i-th channel $(i \in \{h, v, d, a\})$ given that incoming light is $j \in \{H, V, D, A\}$ polarized. Thus to find attack points for the j-th polarization, we choose angles that have higher

values of $\eta_j(j)$ and $\delta_j(j) = \min\left\{\frac{\eta_j(j)}{\eta_{nc0}(j)}, \frac{\eta_j(j)}{\eta_{nc1}(j)}\right\}$, where η_{nc0} and η_{nc1} are the normalized efficiencies of the two detectors in the non-compatible basis. Our experimental attack angles are shown in the rightmost plot in Fig. 2. For example, the H attack angles were composed of points for which $\eta_h(H) \geq 0.2$ and $\delta_h(H) \geq 75$. Similarly, for the V, D and A attack angles, $\eta_v(V) \geq 0.002$, $\delta_V \geq 8$; $\eta_d(D) \geq 0.4$, $\delta_D \geq 80$; $\eta_a(A) \geq 0.1$, $\delta_A \geq 20$. The thresholds used here to find the attack angles were not optimal, and were picked manually.

To derive the key rate and QBER formula in Eve's presence, we start with a system with only Eve and Bob. Let's consider Eve sending an H-polarized pulse to Bob within the attack angles H. Before squashing, the raw click probability $p_i(j)$ that detector i in Bob clicks given Eve has sent j-polarized light is

$$\begin{aligned} p_h(H) &\approx c_h + 1 - \exp\left(-\frac{\mu_H F \eta_h(H)}{2}\right), \\ p_v(H) &\approx c_v + 1 - \exp\left(-\frac{\mu_H (1-F) \eta_v(H)}{2}\right), \\ p_{d(a)}(H) &\approx c_{d(a)} + 1 - \exp\left(-\frac{\mu_H \eta_{d(a)}(H)}{4}\right), \end{aligned} \tag{1}$$

where μ_H is Eve's mean photon number and c_i is Bob's background click probability per bit slot in i-th channel. The probability $P_{hv}(H)$ that after squashing Bob measures in HV basis, given Eve has sent an H-polarized pulse, is composed of three events: when only detector H clicks, when only detector V clicks, or when both click. It can be written as

$$\begin{aligned} P_{hv}(H) = &\big[1 - p_d(H)\big]\big[1 - p_a(H)\big] \\ &\times \big[p_h(H) + p_v(H) - p_h(H)p_v(H)\big]. \end{aligned} \tag{2}$$

Let's now include Alice into the picture. Consider Alice sends an H-polarized pulse, and Eve intercepts it. Let $P_c^e \approx \frac{1}{2}(1 - e^{-\mu F \eta_e}) e^{-\mu(1-F)\eta_e}$ and $P_w^e \approx \frac{1}{2} e^{-\mu F \eta_e}(1 - e^{-\mu(1-F)\eta_e})$ be the probability that Eve measures in the compatible basis (i.e., the same basis as Alice) and gets a click only in the correct and wrong detector respectively. Let $P_{nc}^e \approx \frac{1}{2}(1 - e^{-\frac{\mu\eta_e}{2}}) e^{-\frac{\mu\eta_e}{2}}$ be the probability that she measures in the non-compatible basis (different basis than Alice's) and gets a click in a single detector. The sifted key rate given Alice has sent H-polarized light is

$$\begin{aligned} R_e(H) \approx &P_c^e P_{hv}(H) + P_w^e P_{hv}(V) + P_{nc}^e \left[P_{hv}(D) + P_{hv}(A)\right] \\ &+ (1 - P_c^e - P_w^e - 2P_{nc}^e)(c_h + c_v - c_h c_v). \end{aligned} \tag{3}$$

An error can occur when Eve measures Alice's signal in non-compatible basis or when Eve measures in compatible basis but Bob measures a wrong value owing to imperfect fidelity or dark count. Hence, the error rate conditioned on Alice sending H-polarized light is

$$\begin{aligned} E_H \approx &P_c^e P_v(H) + P_w^e P_v(V) + P_{nc}^e \left[P_v(D) + P_v(A)\right] \\ &+ (1 - P_c^e - P_w^e - 2P_{nc}^e)(c_v - \frac{c_v c_h}{2}), \end{aligned} \tag{4}$$

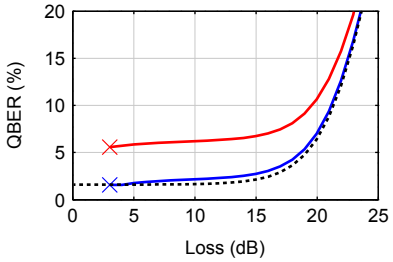

FIG. 3. (color online). Modeled QBER observed by Bob versus line loss. The dotted curve shows QBER without Eve. At lower line loss, the QBER is due to imperfect fidelity, while at higher line loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER_e under our attack when only the total Bob's sifted key rate R_{ab} is matched. The upper solid curve (red) additionally keeps his four channel rates equal.

where $P_i(j)$ is the probability that Bob measures value i after squashing, given Eve has sent j-polarized light. For example,

$$P_v(H) = \big[p_v(H) - \frac{p_h(H)p_v(H)}{2}\big]\big[1 - p_d(H)\big]\big[1 - p_a(H)\big]. \tag{5}$$

Sifted key rates and errors in Eve's presence [Eqs. (3) and (4)] conditioned on V, D, A polarizations sent by Alice can be calculated similarly. The total sifted key rate and QBER in Eve's presence become

$$\begin{aligned} R_e &= \frac{1}{4} \sum_{j=H,V,D,A} R_e(j), \\ \mathrm{QBER}_e &= \frac{1}{4R_e} \sum_{j=H,V,D,A} E_j. \end{aligned} \tag{6}$$

The only free parameters left for Eve to manipulate are the mean photon numbers of her signal. Knowing the angular scanning data, Eve can use a numerical optimization to find values of μ_H, μ_V, μ_D, μ_A that minimize QBER_e while keeping $R_e = R_{ab}$, where R_{ab} is Bob's sifted key rate without Eve. Our numerical optimization achieves this for Alice–Bob channel loss ≥ 3 dB if they are willing to accept a slight increase of QBER by less than 0.7% (see Fig. 3). Here we assumed Bob's detector parameters as measured by us: efficiency at $\phi = \theta = 0$ was 0.4 in all four channels, and individual detector background count probabilities were in the range of 430×10^{-9} to 1560×10^{-9} per 1 ns coincidence window. These optimization results are realistic conditions for a successful attack on most communication channels [14–17, 19, 20, 22, 36] Note that the distance Eve–Bob can be increased without affecting attack performance, by replacing Eve's illuminator with four collimators oriented at the required attack angles.

We went further and imposed an additional constraint on Eve to make $R_e(H) = R_e(V) = R_e(D) = R_e(A) = R_{ab}$. Our optimization shows that it is still possible for Eve to pick appropriate mean photon numbers and

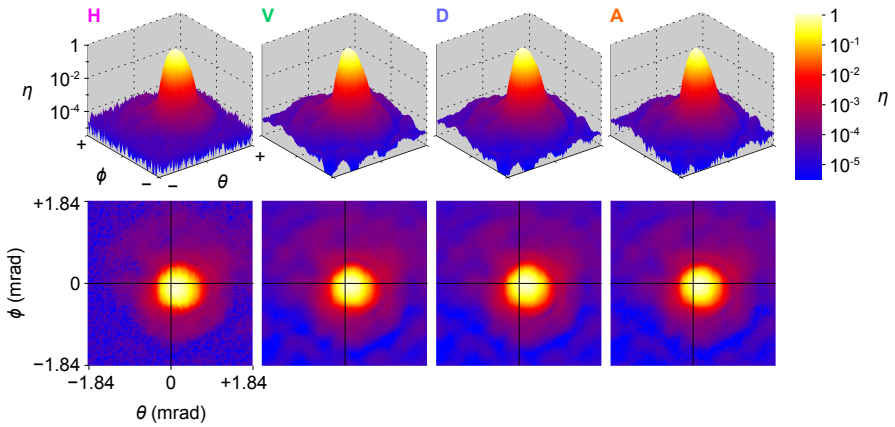

FIG. 4. (color online). Angular efficiency scan of the receiver after a 25 μm diameter pinhole (Thorlabs P25S) is placed in the focal plane of L1, L2 [Fig. 1(a)]. No detectable mismatch between channels was found under tight search conditions $\eta_i(j) \geq 0.001$ and $\delta_i(j) \geq 4$.

successfully attack the system with resultant QBER $<$ 6.82% in 3–15 dB line loss range (Fig. 3). Similar QBER values are typical for outdoor channels, because of background light. Eve could shield Bob from the latter to hide QBER resulting from her attack.

We would like to point out that the attack angles depend on the way the setup is constructed, the imperfections of each individual sample of component, and each individual alignment procedure. I.e., no two setups are identical, even if they are produced in the same assembly line, and they will generally have different attack angles. However, from a theoretical point of view, in quantum cryptography it is assumed from Kerckhoffs' principle [45] that except for the keys themselves, Eve has knowledge about all other parameters in the system. It is thus a valid assumption that she knows the attack angles. From a practical point of view, Eve may try techniques proposed in [40]. She may replace a small fraction of the signal states with faked states at different spatial angles, then listen to the classical communication to get an estimate of the efficiency of Bob's detectors at those angles. In this way she may gradually improve her estimate on the mismatch without causing excessive QBER. When she has enough information on the statistics of the mismatch, she can launch her full-fledged attack.

V. COUNTERMEASURES

In our attack, by sending lights at different angles, Eve has broken a fundamental assumption of security proofs that detection probabilities are independent of detection basis [46, 47]. We propose to restore this assumption by placing a spatial filter (pinhole) at the focal plane of Bob's L1 and L2 [Fig. 1(a)]. Spatial filtering is sometimes done before the beamsplitters to increase signal-to-background ratio in the channel [17, 18, 21], however it has not been characterised as a security countermeasure. We performed scanning with 100, 75, and 25 μm diameter pinholes, and found that decreasing the pinhole diameter gradually reduces the mismatch. The 25 μm diameter pinhole eliminated any visible mismatch (Fig. 4) even though we reduced our search parameters to $\eta_i(j) \geq 0.001$ and $\delta_i \geq 4$. This pinhole provides Bob's field-of-view of 100 μrad, which does not reduce his efficiency with turbulent atmospheric channels [19]. Hence, we conclude that a 25 μm pinhole may be an efficient countermeasure for the current setup.

Note that, in Refs. 29 and 48, a detector scrambling strategy was proposed that might be an effective countermeasure against efficiency mismatch attacks for single-photon qubits. However, it is not clear how effective that countermeasure is, when one considers that the detectors operate on optical modes, not on single-photon signals. This can be a future study.

VI. CONCLUSION

Our analysis implies that data obtained during a QKD session can be explained by an intercept-resend attack exploiting the spatial mode side-channels. Therefore, there is no postprocessing or privacy amplification that can eliminate Eve's knowledge without sacrificing all key [49]. Although our practical attack should work, and the physical countermeasure seems promising, there is still room for improvement on both the attack scheme and countermeasures. Eve can employ more attack angles or combine this attack with some other suitable attack schemes, to increase the number of her free parameters. Alice and Bob can make this harder by monitoring more parameters. We expect that our attack can be conducted also in the related decoy-state protocol [50], though the requirement to match the correct decoy statistics will modify the parameter regime where it will be effective. Another possible future study is to fully implement the present attack under realistic outdoor channel conditions.

ACKNOWLEDGMENTS

We thank Y. Zhang and M. Mosca for discussions. This work was supported by US Office of Naval Research, Industry Canada, CFI, Ontario MRI, NSERC, Canadian Space Agency, and CryptoWorks21. P.C. acknowledges support by Thai DPST scholarship. J.-P.B. and T.J. acknowledge support from FED DEV.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[5] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[8] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, J. Cryptology **5**, 3 (1992).

[9] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[10] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).

[11] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[12] Commercial QKD systems are available for purchase, as of 2015, from at least three entities: ID Quantique (Switzerland), `http://www.idquantique.com`; SeQureNet (France), `http://www.sequrenet.com`; and Austrian Institute of Technology (Austria), `http://www.ait.ac.at/`.

[13] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).

[14] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).

[15] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature **419**, 450 (2002).

[16] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, Proc. SPIE **4917**, 25 (2002).

[17] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).

[18] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, Fortschr. Phys. **54**, 840 (2006).

[19] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. **3**, 481 (2007).

[20] C. Erven, C. Couteau, R. Laflamme, and G.Weihs, Opt. Express **16**, 16840 (2008).

[21] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045007 (2009).

[22] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nat. Photonics **7**, 382 (2013).

[23] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).

[24] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).

[25] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).

[26] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).

[27] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[28] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[29] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).

[30] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).

[31] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001); N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[32] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[33] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).

[34] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).

[35] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, IEEE J. Quantum Electron. **21**, 6600905 (2015).

[36] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. Lütkenhaus, and T. Jennewein, (manuscript in preparation).

[37] R. Tyson, *Principles of Adaptive Optics*, 3rd ed. (CRC Press, 2010).

[38] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, Opt. Express **12**, 2011 (2004).

[39] H. Takenaka, M. Toyoshima, and Y. Takayama, Opt. Express **20**, 15301 (2012).

[40] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[41] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[42] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[43] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **89**, 012325 (2014).

[44] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photonics **7**, 210

(2013).
[45] A. Kerckhoffs, J. des Sciences Militaires **IX**, 5 (1883).
[46] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[47] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[48] T. F. da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, IEEE J. Sel. Top. Quantum Electron. **21**, 1 (2015).
[49] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[50] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).